SANDBAR PERFORMANCE BASED STATEMENT OF WORK (PBSOW)

C.1 BACKGROUND

The Department of Defense (DoD) and its Interagency Partners require support across a broad range of technical and engineering tasks for the design, development, and sustainment of specialized information technologies (IT) as well as full system development lifecycle support for global systems and network architectures. This support includes engineering to enhance operations, sustainment, integration, and improvements to systems and networks.

C.1.1 PURPOSE

This Performance Based Statement of Work (SOW) provides the Department of Defense (DoD) and Interagency Partners with services that support the development, integration, operation, and sustainment of classified cyber operations infrastructure capacity and related services.

C.2 SCOPE

The scope of this performance based SOW includes lifecycle system and capability support to include the research, design, test, deployment and sustainment activities supporting DoD, and its interagency partners. In support of the effort the contractor shall:

Task 1: Provide Program Management: This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW).

Task 2: Provide System Design: The Contractor shall perform engineering and system design support across multiple engineering and technical disciplines for the development of improvements to existing Command, Control, Communications, and Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and Information Technology (IT) capabilities and systems. The Contractor shall design capabilities for critical missions which include alterations to existing systems; integration and enhancements to systems and other system component interfaces; and development and modifications to new and existing software systems.

Task 3: Provide Research Support: The Contractor shall provide advanced system research, development, test, and evaluation and specialized system support. This shall include access to multiple subject matter experts in a variety of technical domains including telecommunications, security engineering, and information assurance.

Task 4: Support System Development: The Contractor shall be responsible for all engineering and development tasks required to build and test system capabilities and ensure the desired outcome can be traced back to design requirements. This may be an iterative process where feedback and interim results are reviewed prior to completion.

Task 5: Provide Test and Evaluation Support: The Contractor shall establish a

rigorous independent T&E program that evaluates the correctness and quality of a technology or system to ensure that it is being developed in accordance with DoD requirements and is well-engineered. Independent Verification and Validation (IV&V) efforts provide high value to many projects and may be introduced at any phase of a project as determined by the project's sponsorship and/or Operating Division's governance requirements.

Task 6: Support Deployment of Capability: The Contractor shall be responsible for system deployment to end users where newly completed systems or capabilities are fielded. It shall include planning, scheduling and communication with stakeholders and end users to ensure that new systems or capabilities are deployed to production environments in a controlled manner to minimize risk.

Task 7: Support Capability Sustainment: The Contractor shall provide advanced system engineering, network administration support, and security services support to ensure system operational reliability and maintainability.

Task 8: Provide Capability Integration: The Contractor shall assist the Government with detailed technology roadmaps and transition planning and master plans as required. The Contractor will support the transition of systems to a wider acceptance and integration within the Government on technologies and systems identified as priorities for moving from prototypes to wide-scale system integrations programs. This includes both hardware and software-based solutions.

Task 9: Provide Accreditation Support: The Contractor shall provide cybersecurity compliance, Information Assurance (IA) oversight & management, certification and accreditation, and the required security support services for current and future systems maintained under this contract. These services shall be delivered using a systematic disciplined approach to the evaluation of risk management, information security controls, and governing processes.

Task 10: Provide Support to Special Acquisitions: The Contractor shall assist the Government in the specialized acquisition of hardware and software from vendors using established mechanisms. These mechanisms shall also be used to provide engineering support to ensure appropriate-attribution and counter intelligence safeguards.

Task 11: Provide Training Support: The Contractor shall be responsible for both user and system administrator training. Training presentations shall be prepared for the customer to review and approve. Once approved, training classes shall be scheduled and delivered so that all users and system administrators have the training they need to get full use of all deployed systems.

C.3 OBJECTIVE

The Objective of this contract is to support the following activities:

a. Maintain, sustain, and oversee systems and provide advanced technical support and operational expertise
b. Expand system and network architectures

c. Extend the current architecture across service components
d. Create and expand new technologies and configurations to support new mission requirements
e. Improve and harden existing system architectures and specific system technologies
f. Update and improve the command and control components
g. Provide specialized acquisition support for hardware and software from vendors
h. Integrate and test new technologies and capabilities
i. Provide system and technology training support as required

C.4 TASKS

C.4.1 TASK 1 –PROJECT MANAGEMENT

The contractor shall provide project management support under this effort. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this performance based SOW. The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this contract.

C.4.1.1 SUBTASK 1 –PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (Section F, Deliverable 2). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the contract. The meeting will provide the opportunity to discuss technical, management, and security issues, as well as travel authorization and reporting procedures. At a minimum, the attendees shall include Key Personnel, other contractor support personnel, representatives from the applicable DoD directorates, other relevant Government personnel, and the COR.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 1) for review and approval by the COR and the Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties
b. Draft Project Management Plan (PMP) (Section F, Deliverable 7) and discussion including schedule, tasks, etc.
c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government)
d. Staffing Plan and status
e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs))
f. Invoicing considerations
g. Transition discussion
h. Final Baseline Quality Control Plan (QCP) (Section F, Deliverable 12)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 3) documenting the Kick-Off Meeting discussion and capturing any action items.

C.4.1.2 SUBTASK 2 – MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (**Section J, Attachment D**) (Section F, Deliverable 4). The MSR shall include the following:

a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
g. Total subcontracting during the reporting period, itemized by subcontractor and associated dollar value.
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.

C.4.1.3 SUBTASK 3 – MONTHLY TECHNICAL STATUS MEETING

The contractor PM shall convene a monthly Technical Status Meeting with the TPOC, COR, and other Government stakeholders (Section F, Deliverable 5). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting (Section F, Deliverable 6).

C.4.1.4 SUBTASK 4 – PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 7) on which the Government will make comments. The final PMP shall incorporate the Government's comments.

The PMP shall:

a. Describe the proposed management approach.
b. Contain Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this contract.

d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
e. Describe in detail the contractor's approach to risk management under this contract.
f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
g. Include the contractor's Baseline QCP.

C.4.1.5 SUBTASK 5 –QUALITY CONTROL PLAN (QCP)

The contractor shall develop and maintain a QCP, updating as required (Section F, Deliverable 11). The QCP shall be updated as changes in program processes or standard operating procedures occur.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the contract. The contractor's QCP shall describe its quality control methodology for accomplishing contract performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each task area. The QCP shall describe how the contractor's processes integrate with the Government's requirements.

C.4.1.6 SUBTASK 6 – FINANCIAL MANAGEMENT

The contractor shall provide financial management and reporting by CLIN and include subcontractor financial data. The contractor shall provide supplemental reporting as required to include: resource planning; cost reporting; impacts assessments; invoicing; and disclosure requirements.

C.4.1.7 SUBTASK 7 – PRESENTATION MATERIALS

The contractor shall conduct, support, and lead presentations. The contractor shall provide material for meetings at times and places to be determined with the Government and Contractor. Any final presentation materials that will be retained and recorded in the Government file shall be due within five days after the presentation. (Section F, Deliverable 14)

C.4.1.8 SUBTASK 8 -TRANSITION-OUT

The contractor shall provide Transition-Out support and develop a Transition-Out Plan, which facilitates the accomplishment of a seamless transition from the incumbent to an incoming contractor and/or Government personnel at the expiration of the contract. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS) (Section F, Deliverable 15).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition

f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless Transition-Out.

The contractor shall implement its Transition-Out Plan NLT three months prior to expiration of the contract.

C.4.1.9 SUBTASK 9: ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the US Army via a secure data collection site. The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.4.2 TASK 2 – SYSTEM DESIGN

The Contractor shall provide engineering and system design support for the development of improvements to existing C4ISR and IT capabilities and systems (specifically classified cyber operations infrastructure). The Contractor shall design capabilities for critical cyber operations, which include alterations to existing systems; integration and enhancements to systems and other system component interfaces; and development and modifications to new and existing software systems. The Contractor shall perform technology and engineering analysis and evaluation of foreign systems, equipment, and technologies. These efforts are necessary to design and transform operational needs into unique system capabilities with performance parameters needed to support rapidly evolving customer missions.

The Contractor shall perform design activities in support of new capability development that can be integrated into cyber operations infrastructure. Design activities will include customer needs assessments and requirements definition. The Contractor's system design efforts shall detail how defined requirements will be implemented into the system. Design specifications shall include how the system, component or new capability will be architected and built, as well as how the system will be integrated within the existing systems architecture or interfaced with external systems as applicable. The design activities include conducting fit/gap analysis, developing overarching technical architectures, and detailing specific functional elements and dependencies.

C.4.3 TASK 3 – RESEARCH

The Contractor shall provide advanced system research, development, test and evaluation, and specialized system support to increase cyber operations infrastructure capability and capacity. This shall include access to providing multiple subject matter experts in a variety of technical domains including telecommunications, security engineering, and information assurance.

The Contractor shall perform extensive engineering, technical, and operational analytical support services. This includes performing in-depth technical assessments of vendor solutions, malware reverse engineering, network and cloud analytics, emerging technology assessment and analysis, Independent Verification & Validation (IV&V) and a host of research, development, test, and evaluation (RDT&E) support requirements. Analytic support and research shall be performed on Commercial off-the-shelf (COTS) and Government off-the-shelf (GOTS) applications as well as emerging technologies that are still in the development phase. The Contractor shall be responsible for the assessment of new technology and solutions by performing research and preparing for proper technology deployment, security measures adherence, technology interoperability, system resource management, system de-confliction, and user allocation. The contractor shall provide detailed and comprehensive engineering and analytical support. The Contractor shall be required to provide this analytic support as part of a team effort across multi-vendor and multi-Government organizations.

C.4.4 TASK 4 – SYSTEM DEVELOPMENT

The Contractor shall provide all engineering and development tasks required to build and test cyber operations infrastructure system capabilities and ensure the desired outcome can be traced

back to design requirements. This may be an iterative process where feedback and interim results are reviewed prior to completion.

The Contractor shall provide highly specialized system and network engineering services in support of the development of next generation cyber operations infrastructure systems and network infrastructures. The Contractor shall perform extensive system, network and software engineering, and technology validation and integration.

Contractor shall operate and maintain contractor secure laboratories for system operations testing. The Contractor shall also provide operations and sustainment services for their own provided global network. All network services provided shall be through vetted vendors and with closely managed attribution. Prior to incorporating services into Government operations, the Contractor shall deploy active defense tools using tradecraft in order to have full operational awareness over all managed platforms and services. These services shall be performed at both Government sites and at Contractor locations. The Contractor shall provide tiered Network Operations/Secure Network Operations (NOC/SOC) support and problem remediation. The Contractor shall support end user operations as well as network security operations that include monitoring and detection to identify potential adversarial activities.

The Contractor shall develop unique capabilities and web-based solutions, which are required for the automation and optimization of network operations in support of cyber operations. Software engineering shall span the entire Operating System (OS) model to include mobile and wireless devices and from host/server to advanced cloud and web-based systems. The Contractor shall modify, enhance, and/or remediate software code and applications from a wide range of commercial vendors to ensure system certification, accreditation, and effectiveness. The Contractor's solutions shall be centered on improving system performance while decreasing operations, maintenance, and sustainment requirements to ensure system affordability.

The Contractor shall provide engineering services to extend and expand existing system architectures. Expansion will include the adoption and integration of new technologies and systems that will provide enhanced operational capabilities. This support shall include adding new nodes and components to existing systems as well as integrating new technologies and capabilities. New nodes and components shall include CONUS and OCONUS nodes, versatile nodes that are acquired, and more disposable node components to support temporary operational needs. The Contractor shall maintain both the existing as well as new components added to the system. The Contractor shall integrate various technologies such as advanced Cloud Architectures, specialized virtualization software, and Cloud Command, Control, Communications, and Computer (C4) applications and supervisory controls and associated applications into existing systems.

The Contractor shall provide engineering support to update and improve existing cyber operations infrastructure systems, as required. The requested improvements may include the following:

a. Network security upgrades

b. System hardening

c. Command and control software additions and improvements

d. Security component software additions and improvements

e. Integration of new, more secure, and more advanced routing elements.

C.4.5 TASK 5 – TESTING AND EVALUATION

The Contractor shall provide technical and engineering support, which includes establishing a rigorous independent T&E program that evaluates the correctness and quality of a technology or capability to ensure that it is being developed in accordance with DoD requirements IV&V efforts provide high value to many projects and may be introduced at any phase of a project as determined by the project's sponsorship and/or Operating Division's governance requirements. Note that depending on project size, risk and other operational factors, the DoD will determine the appropriate scale of IV&V activities and can approve tailoring the IV&V requirements to match the program and operational requirements. The Contractor shall ensure adequate independence of verification and validation to include utilization of firewalled third-party evaluators and/or an adequately firewalled evaluation team, as coordinated with and approved by the Government (for each verification and validation effort). The Contractor shall ensure appropriation coordination with Government verification and validation, as applicable.

The Contractor shall establish a T&E process, which includes but is not limited to IV&V reviews, analysis, evaluations, inspections, and tests of the project's technical capabilities, system behaviors, processes and interfaces, operational use, feasibility or practicality of the technology in a given operational environment, and durability of the system as examples.

The Contractor shall establish a Rapid IV&V program to allow for rapid system fielding by conducting streamlined testing and analysis. Each test shall include the operational environment (as close as possible), consisting of any hardware, software, interfacing applications and systems, documentation, operators, and user experience to ensure that the product is well-engineered, and is able to be deployed and developed in accordance with DoD requirements.

The Contractor shall develop an IV&V program, which provides the DoD with an independent perspective on project activities and promotes early detection of project/product variances. This allows the project to implement corrective actions to bring the project back in-line with agreed-upon expectations. Objectives of performing IV&V include:

a. Facilitate early detection and correction of cost and schedule variances
b. Enhance management insight into process and product risk
c. Support project life cycle processes to ensure compliance with regulatory, performance, schedule, and budget requirements
d. Validate the project's product and processes to ensure compliance with defined requirements

IV&V findings and reports provide supporting evidence that the product does satisfy client requirements. IV&V should be performed throughout the project's life as applicable and can be executed incrementally at specific points in the life cycle or be performed in a manner that is integrated into all project efforts.

C.4.6 TASK 6 – DEPLOYMENT

The Contractor shall be responsible for cyber operations infrastructure system deployment to end users where newly completed systems or capabilities are fielded. This shall include planning,

scheduling and communication with stakeholders and end users to ensure that new systems or capabilities are deployed to production environments in a controlled manner to minimize risk.

Activities shall include:

a. Installation of system software, hardware, and network infrastructure components
b. Development of documentation describing component build/installation/configuration
c. User acceptance testing as required
d. End user training
e. Delivery of end user support and training materials
f. System hand-off and customer signoff
g. Transition to support

C.4.7 TASK 7 - SUSTAINMENT

The Contractor shall provide advanced system engineering, network administration support, and security services support to ensure cyber operations infrastructure system operational reliability and maintainability. The contractor shall support providing data and system integrity. These services shall include but are not limited to:

a. Monitor all system nodes and associated components
b. Analysis of security and administrative logs
c. Upgrade system components with security patches
d. Engineering remediation activities to mitigate potential vulnerabilities
e. Configuration Management
f. Lifecycle Management

The Contractor shall continue to operate, maintain, and upgrade all hardware, firmware and software built into systems to ensure cyber operations infrastructure system security and integrity. All software and firmware upgrades are required to ensure system security shall be executed in a timely fashion. The contractor shall maintain an inventory of all hardware and software components and their configurations. A configuration management process shall be used to ensure all of these actions and data are tracks, tested, approved, and implemented using and planned and measures process.

The Contractor shall apply configuration management to identify, document, and verify the functional, performance, and physical characteristics of systems and associated interface systems, to control changes and non-conformance, and to track actual configurations of systems and platforms. The Contractor shall apply configuration management throughout the system development lifecycle and sustainment operations.

The Contractor shall ensure all elements of systems under configuration control are managed and tracked, while staying agile enough to meet operational requirements. The

Contractor's configuration management process shall ensure only approved and vetted changes are made to systems, enabling personnel to ensure assets are in their properly configured state and in their proper place within the system.

As part of the operations and maintenance support the Contractor shall perform continuous monitoring and reporting via a NOC on all equipment and all network traffic into and out of system networks. NOC support shall be provided in a tiered fashion to provide basic functions such as proactively monitoring all network circuits, systems, and servers and troubleshooting/triaging trouble tickets, to SMEs that provide detailed engineering and support to the operations and sustainment of the infrastructure.

The Contractor shall be responsible for network security operations, system backup systems, all system maintenance, trouble ticketing system, help desk functions, emergency management, and all system technology remediation issues and problems. Reports shall be generated daily and compiled on a weekly and monthly basis. Reports shall be reviewed by the Contractor to ensure the system is stable and there are no unexplained operational problems.

C.4.8 TASK 8 - INTEGRATION

The Contractor shall assist the Government with detailed technology roadmaps and transition planning and master plans as required. The Contractor shall support the transition of systems to a wider acceptance and integration within the Government on technologies and systems identified as priorities; moving from prototypes to wide-scale system integrations programs. This includes both hardware and software-based solutions.

The Contractor is responsible for aiding in transitioning vendor systems to the provided infrastructure, in addition to supporting the development testing, operational testing, and integration testing, and assisting the Government with detailed technology integration assessments and impact analyses.

The Contractor shall develop and maintain a capability to recreate existing cyber operations infrastructure system and network functionality and provide a platform that supports training of operators and testing of new capabilities. This cyber operations architecture shall also help to ensure that good tradecraft is integral to all operations involving any capability to be deployed. This duplicate testing environment shall be designed to ensure reskilling can occur without any negative impact on the operational system. The testing and modification of existing and new tools and capabilities in an environment indicative of the operational one is critical to successful execution and usage.

The Contractor shall support testing, training, and the integration of capabilities into the cyber operations architecture. To fully support these requirements, the cyber operations architecture must also mimic the Internet and its inherent potential for instability. Technologies shall be developed and integrated that can generate different types of network traffic, create network congestions, and create failures throughout different points within the network. These shall work together to support recovery scenarios and configurations within the network as well as verify tool execution and operators' training is sufficient. To ensure that these various network issues can be controlled as needed

during training, testing, or exercises, interfaces shall also be developed that allow for command, control, and status of all of these new technologies.

C.4.9 TASK 9 – ACCREDITATION

The Contractor shall provide cybersecurity compliance, Information Assurance (IA) oversight & management, certification and accreditation, and the required security support services for current and future systems maintained under this contract. These services shall be delivered using a systematic, disciplined approach to the evaluation of risk management, information security controls, and governing processes.

The Contractor shall provide accreditation support based on the Risk Management Framework (RMF), applying risk management throughout the system lifecycle to identify, implement, assesses, and monitor all applicable security controls. The Contractor shall author and develop all RMF artifacts required in support of accreditation including the Security Plan (SP), Security Assessment Report (SAR), Security Controls Traceability Matrix (SCTM), and POA&M.

The Contractor shall provide an Information System Security Officer (ISSO) to lead all IA efforts and act as the single point of contact for information system security matters for all stakeholders. The ISSO shall plan, execute and monitor the systems' security posture and be supported by an Engineering team which provides a wide spectrum of RMF support including IV&V, configuration management, remediation, and documentation. The Contractor shall design, develop, build, remediate and test systems to meet security controls and ensure cyber operations infrastructure systems are configured in accordance with applicable STIGs.

Security controls shall be implemented consistent with DoD IA architectures and policies, employing standard system engineering methodologies and security engineering principles. The Contractor shall follow DoD STIG, IAVA compliance, and NIST 800-53 standards to prevent and identify vulnerabilities and implement corrective actions.

C.4.10 TASK 10 – SPECIAL ACQUISITION

The Contractor shall assist the Government in the development of securitized, non-attributable, and/or anonymous cyber operations infrastructure through the specialized acquisition of hardware and software from vendors using established mechanisms. These mechanisms shall also be used to provide engineering support to ensure appropriate-attribution and counter intelligence safeguards.

The Contractor shall provide a wide range of non-traditional IT related service offerings including the provisioning, acquisition, management, monitoring, operations, and maintenance of these non-traditional type IT service offerings. The Contractor's IT service offerings shall be included directly as part of its purchasing methodology. The Contractor shall install, maintain, and operate all associated IT equipment to any of the client-designated locations in order to properly mitigate the risks of untended attribution to either the Contractor or the Government.

C.4.11 TASK 11 – TRAINING

The Contractor shall be responsible for both user and system administrator training in support of cyber operations via the established and supported infrastructure. Training presentations shall be prepared for the customer to review and approve. Once approved, training classes shall be scheduled and delivered so that all users and system administrators have the training they need to get full use of all deployed systems. Training shall be a combination of in-classroom presentations, on-site individual sessions at appropriate USG working areas, and virtual sessions (where appropriate).